

JUNE 1998
Issue 18



International Journal of
FORENSIC COMPUTING™

Contents

Comment	page 2
News	page 3
Product news	page 10
CompuServe trial	page 14
UK Encryption policy	page 18
DIVA - computer evidence	page 19
Notice board	page 23

- **John Austen**
Computer Crime Consultants Ltd & Royal Holloway College, University of London, UK
- **Jim Bates**
Computer Forensics Ltd, UK
- **Alexander Dumbill**
King Charles House Chambers, UK
- **Ian Hayward**
Former lecturer, Department of Information Systems, Victoria University of Technology, Australia
- **Robert S Jones**
Computer Related Crime Research Centre, Queen Mary & Westfield College, University of London, UK
- **Nigel Layton**
Quest Investigations Plc, UK
- **Stuart Mort**
DRA, UK
- **Michael G Noblett**
Computer Analysis Response Team, FBI, US
- **Howard Schmidt**
Director of Information Security, Microsoft Corp. Former Director of US Air Force Office of Special Investigations Computer Forensics Laboratory
- **Gary Stevens**
Ontrack Data International Inc, US
- **Ron J Warmington**
Citibank NA, UK
- **Edward Wilding**
Network International Ltd, UK

Editorial Team

- **Paul Johnson**
Editor
- **Sheila Cordier**
Managing Editor

International Journal of Forensic Computing

Third Floor, Colonnade House,
High Street, Worthing,
West Sussex, UK
BN11 1NZ

Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail: ijfc@pavilion.co.uk
<http://www.forensic-computing.com>

Anyone who has followed the trial of former CompuServe manager Felix Somm will have been astounded and confused by the recent verdict.

Somm, the former manager of the Internet giant, was found guilty of distributing online pornography. The Bavarian province had singled him out as being personally responsible for the notorious alt Usenet newsgroup hierarchy, which at the time contained hardcore pornography, Nazi symbols and anti-Semitic messages, all of which are banned in Germany.

Yet after four weeks of hearings, even the prosecutors had swung over to the defence view that Somm was not liable under a multimedia law the German parliament passed last August and had called for him to be acquitted.

The law says Internet access providers like CompuServe are not liable for illegal content if they do not have the technology to block the material.

And the defence pointed out that such technology was not available until December 1996. The conviction related to 1995 and 1996, when Somm was head of CompuServe's German division.

The case has been widely seen as a test of attempts to police the Internet, where content can flow freely across borders, but the decision shocked legal and online experts who had called for Somm's acquittal.

No one can deny that a vast amount of deeply unpleasant and undesirable material flows freely on the Net and that anything that can be done to stem this torrent is desirable. But this prosecution is exactly how not to go about it. Knee-jerk reactions like the Somm trial are not only unconstructive by targeting scapegoats, they are actually counter produc-

tive because they set the whole field of forensic computing and prosecution back a great deal.

It is already hard enough for any police force to obtain the equipment and manpower to investigate computer crime when managers would prefer to put cash into tackling "real world crimes". The results of the CompuServe trial can only damage the reputation of such cybercops.

If an Internet service provider knowingly carries illegal material and has the capability to block it, then yes, perhaps it should be prosecuted if it refuses to comply. Obviously there are the added complications of international jurisdiction where material is illegal in one country but not another, but that is another can of worms altogether.

The point is, ISPs are just the conduit, not the originator. Those responsible for the material in the first place – the racists, bigots, paedophiles and perverts – are the ones who should be investigated and prosecuted.

At the moment technology is only catching up with hunting down such online criminals – people can easily cover their tracks on the Net – but when police forces across the world have the right resources and know-how this has to be the ultimate goal.

Until then people like Somm will act as easy targets – scapegoats for authorities to attempt to show just how seriously they view illegal activities on the Internet. There is a huge danger the police and courts – in whatever country – will merely end up as a laughing stock for passing ludicrous judgements.

Meanwhile an army of insidious and dangerous people can carry on peddling their filth unhindered, wrecking who knows how many lives.

All rights reserved. Without prior permission of the Publisher, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise.

Articles are published on the understanding that publication is not taken to imply endorsement of the views therein by the Publisher or Editorial Team or members of the Advisory Board of the Journal. Courses of action described in the Journal in relation to one set of circumstances will not necessarily be appropriate for a different set of circumstances.

Accordingly, readers should take their own independent specialist advice before proceeding on any project or course of action and any failure to do so is at their own risk. No responsibility is assumed by the Publisher or Editorial Team or members of the Advisory Board for any loss or damage to persons or property as a matter of contract, negligence (save in respect of liability for death or personal injury arising out of any negligence) or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Whilst all reasonable care is taken, neither the Publisher, nor the Editorial Team, nor members of the Advisory Board can be held legally responsible for any errors in articles or listings. Upon submission of an article, the author will be requested to transfer copyright of the article to the Publisher.

Anti-virus firms fight back over report

Two competing anti-virus firms have teamed up to dismiss a report that their products are ineffective and erratic.

Sophos and Dr Solomon's issued a joint response to dispute assertions made by Reflex Magnetix that most anti-virus scanners on the market fail to live up to the manufacturer's claims.

Reflex said that the effectiveness of the world's leading anti-virus scanners has been put in doubt by tests conducted over the last two years by BrownWright, an independent consultancy.

Sophos and Dr Solomon's say they have been denied details of where the products failed and details of Web sites where the viruses were obtained.

The firms attacked the report for causing unjustified fear and uncertainty, and accused Reflex of scaremongering.

According to the two companies, the BrownWright report styles itself as an independent summary of a number of anti-virus product reviews across 6,301 viruses. The tests were conducted on unverified files from 20 Web sites claiming to have viruses for download. The report claimed that anti-virus products have "astonishing shortcomings."

"Anti-virus vendors carry out verifiable quality assurance tests of their own," said Paul Ducklin, Sophos' head of research, who added that tests such as those carried out for the BrownWright report only serve to encourage users not to take anti-virus testing seriously.

Windows NT e-mail "not secure"

Almost a quarter of all UK firms using Windows NT based e-mail are open to attack from hackers, according to IT security firm NTA Monitor.

The bottom line to this, the firm says, is that such users are risking catastrophic consequences as the result of taking no security precautions.

NTA Monitor bases its assertion on a major survey carried out across the Internet, in which it says it interrogated 1,231 UK Web sites that used Windows NT to host their e-mail servers. The elec-

tronic interrogation survey found that 23 per cent of sites are compromising their confidentiality, because simple, low cost security measures have not been taken to protect the systems from abuse.

The company says that the security risks are caused by the sites not screening Windows NT's NetBIOS over TCP/IP function of their servers, which can be done at no cost in the site's Internet router, or in a typical firewall.

According to NTA Monitor, access to the NetBIOS can result in several problems, including the fact that any third party accessing privileged information on the server can be intercepted. This could be user accounts, lists of other machines on the network, details of any hard disk drives that are being shared, and any other workgroups the server is aware of.

NTA also says that any third party logging in to the Web site anonymously - with no account name or password needed - can discover even more information about the server.

This alone does not allow full access, the company says, but does enable the attacker to make changes to the Windows Registry to open other access holes. Such changes, the company says, come into force the next time the server is restarted and the server is then well and truly in the hands of the attacker.

NTA's survey also discovered that the most popular NT mail software in use is NT Mail, claiming 52.3 per cent of the market share, with Microsoft Exchange being used at 25.6 per cent of the sites, and Mimesweeper, VirusWall, and NASTA following close behind.

Deri Jones, NTA Monitor's managing director, said he finds it astounding that so many sites have taken no action whatsoever.

He said: "Despite all the media attention given to security, many organisations are still missing out on basic perimeter security. Companies risk having their e-mail, both in and outbound, picked up by third parties.

"Even worse, they are open to the injection of libellous e-mails into the Internet from their systems, so that it is impossible to prove after the event that they were not created by staff - a disastrous source of potential litigation."

Jones says that the risks are not just to their e-mail servers, as the information leaked by NetBIOS about other machines in the company provides an ideal start for an attacker to mount a "stepping stone attack" further into the company, and gain access to more systems.

"The only way to entirely protect an organisation's NT Internet servers from this vulnerability is to block the NetBIOS in the perimeter protection, which can be easily achieved in even the most basic of Internet connections.

"The message cannot be much simpler - companies should test their Internet security systems, before they get caught out," he said.

To help users, the firm is now offering a free test to organisations wanting to check the vulnerability of their NT Internet servers. To take part, users are asked to send an e-mail to netbios-tests@nta-monitor.com, including details of the company's name, contact, and fax number in the body of the message.

According to NTA Monitor, it ran a series of live tests between December of last year and May of this, across the Internet - contacting each of the 1,231 active mail server machines running Windows NT in the UK's "co.uk" Internet domain space.

NTA Monitor's web site is at <http://www.nta-monitor.com>

Senate committee passes copyright bill

International copyright protection moved a step closer to reality, as the US Senate Judiciary Committee unanimously approved legislation to ratify two World Intellectual Property Organisation treaties designed to enforce international copyright protections in cyberspace.

"It's wrong to encourage an electronic marketplace in stolen goods," Recording Industry Association of America President Hilary Rosen said, "and that's what we'll have without these treaties and the implementing legislation."

The legislation passed by the Judiciary Committee parallels legislation in the US House of Representatives, which is awaiting scheduling for a vote by the full House, but with significant compromises to the online and recording industries.

That legislation, HR 2281, and introduced by Rep. Howard Coble (R-North Carolina), also would prohibit knowingly providing false copyright management information with intent to induce or conceal software piracy and other copyright infringement.

This would protect Internet service providers (ISPs) from copyright infringement for unknowingly distributing unauthorised copyrighted material.

The copyright treaty will protect copyrighted material in the digital environment, including the Internet, Coble said, while the performances and phonograms treaty will provide stronger international protection to performers and producers of phonograms.

Efforts by telephone company interests to gain exemptions from liability from copyright infringement on the Internet, however, have slowed its progress in both chambers, leading to the compromise in the Senate.

Under the Senate's compromise legislation, Internet service providers, as well as telephone companies, would be protected from copyright infringement liability if users illegally transmit or post copyrighted works online without the knowledge of the service provider.

Internet service providers, however, still could be sued if they knowingly allow copyright infringements on their services, or if they profit from the illegal use of copyrighted materials.

Australia's Internet copyright laws

Commonwealth Attorney-General Daryl Williams says that new copyright laws will make Australia a leader in the Internet world.

The changes include a technology-neutral right of communication to the public which would apply to works available on the Internet, as well as works transmitted or broadcast by more conventional means.

Picking up a theme from recent US Federal Court judgements, Williams said the Copyright Act will ensure telcos and Internet service providers will not be liable for copyright infringements on their customers' Web sites.

Exceptions to copyright for fair dealing, libraries and educational institutions would continue.

Williams said the reforms should ensure copyright owners were "appropriately rewarded" for the use of their books, software, art and music, while reassuring the community it would continue to have reasonable access to those works on the Internet.

CompuServe's Crimebuster forum

CompuServe's UK operation has launched a crimebusters forum for its subscribers.

Known as the UK Police and 999 Emergency Services forum, the service has been established following the success of the UK Professional and UK Medical forums on CompuServe, which the service says have attracted high usage by emergency services staff, particularly members of the UK police force.

According to CompuServe officials, subscribers can now increase their awareness of UK crime prevention methods and make important contributions to community policing by taking part in the new forum, as well as being able to exchange online views with real members of the police force.

The forum has both public and private areas. The private areas include ones for police officers and for the International Police Association.

The public ones, meanwhile, include areas such as "Ask the Police," where members of the public can ask all sorts of questions, ranging from "How do I join the local Neighbourhood Watch Scheme?" to "How do you join the Police Force?"

Alternative sections cover other elements of crime prevention, as well as a file library, where users can download information files covering most aspects of policing in the UK, as well as bulletins from the FBI.

CompuServe has appointed Jim McNulty, a retired Glasgow detective, as the UK Police forum sysop. He said that the forum is already proving its value in terms of communication between officers and the public.

"People chat to the officers, ask questions, and generally gain a better understanding of policing. Officers in turn obtain very frank feedback in relation to concerns and perceptions which the public have," he said.

According to McNulty, "Such an exchange can only lead to a better understanding of policing needs by all concerned."

To access the forum, CompuServe subscribers should issue the command GO UKPOLICE. Web users of CompuServe can go to <http://www.compuserve.co.uk>.

Anti-piracy Web site

In its continuing campaign against software piracy, the Business Software Alliance has opened up an IT professionals Web site to help managers fight fraud in the workplace.

"Copying software is so easy that anyone can do it - yet it is the IT managers who are blamed and their profession damaged. We want IT managers to know that they do not have to accept this anymore - they need no longer be held ransom to other people's ill-considered actions," said Tracey Howe, the BSA's chairman.

According to Howe, the new anti-software theft site provides IT managers with a number of tools that will help them communicate the serious implications of using illegal software to staff and senior management.

Howe said that the BSA developed this initiative after canvassing for opinions among IT professionals and found that they would welcome support that would help maintain a legitimate and professional system and avoid the administrative hazards that accompany the use of unauthorised software.

The Web site provides IT managers with the facility to download a variety of information tools. Employee communication templates suggesting an outline company policy for the use of personal software on the network can be used by IT managers.

There are also contact details for ordering the "Two Minute Assessment" form that will alert them to any shortfall in licenses and give guidance on re-

medial options available.

The site, at <http://www.nopiracy.co.uk>, is linked to the main BSA Web site at <http://www.bsa.org>

Law enforcement gets high-tech tools

State of the art technology will be developed to help law enforcement agencies in the US combat the threat of cyber crime.

"If we're going to fight the criminals of the future, we need to develop the crime fighting tools of the future," Vice President Al Gore said as he announced the Energy Department will work closely with the Departments of Justice and Treasury to develop new systems.

"We must put the best possible tools in the hands of our law enforcement community so they can identify, apprehend, and prosecute criminals swiftly and effectively," Gore said.

Gore, joined by Energy Secretary Federico Pena, Treasury Secretary Robert Rubin, Attorney General Janet Reno, and state and local law enforcement representatives, announced a "Partnership for a Safer America" at a demonstration of cutting-edge crime fighting technology.

The technologies demonstrated today included an image analysis and video enhancement technology developed by the Energy Department's Oak Ridge National Laboratory.

The Oak Ridge technology, Gore said, was used by the Chattanooga, Tennessee Police Department to isolate the gun flare in a convenience store shooting videotape.

The evidence provided by the technology, Gore said, resulted in a first-degree murder guilty plea and a life without parole sentence, he said.

Secretary Pena added that "hand-held geographic positioning devices that can record video and store voice notes can help agents visually reconstruct crime scenes.

"Crime is becoming increasingly high-tech," Pena said, "from Internet predators to sophisticated bomb builders. But today, we have a message to

criminals, 'Beware, because we are going to come after you with technologies you've never seen before.'"

Gore, speaking at the 17th annual Peace Officers Memorial Services, also announced that two Energy Department Memoranda of Understanding were signed with the FBI and with the Bureau of Alcohol, Tobacco, and Firearms.

Under the MOUs, Gore said, the Energy Department "will establish formal working relationships to facilitate the transfer of technology and technical expertise to law enforcement."

A Statement of Principles also has been prepared between the Energy, Justice and Treasury Departments, he said, "to co-ordinate and facilitate the technical advancement of crime fighting in this country."

Pena said that, in support of the principles, the Energy Department has selected a number of technologies from the Department's seven national laboratories for "further collaborative development."

"These technologies are core DOE competencies that will provide future forensic and crime scene investigation tools, as well as examples of actual DOE laboratory technology or expertise being used by law enforcement," he said.

Among the technologies are portable chemical analysis machines to gather evidence from crime scenes, and a number of software programs designed to help trace online crime.

China vulnerable to hackers

Chinese computer networks are almost certain to be breached by hackers, according to network security vendor Security Dynamics.

Speaking at a Hong Kong network security seminar, Chief Operating Officer Arthur Coviello said that a near universal reliance on reusable passwords left local networks wide open to abuse.

A Western hacking group calling itself the Ministry of Downloading recently threatened to attack Chinese computer networks, after a series of widely publicised breaches of US military sites.

Director of technical marketing, Marc Fastiggi, said successful attacks on

Chinese networks could be expected. "I would say that it's almost a certainty that you've had attacks in China," he said. "Most of the holes that the hackers use are the same worldwide."

Coviello said China, which imposes strict restrictions on encryption tools, was particularly vulnerable to attacks.

"Whatever is the highest level of privilege that you allow in your firewall is the level at which the hacker is going to get through," he said.

"If you keep the technology away from business and limit its exposure then it's the criminal element that will find a way of using it."

Security Dynamics manufactures some of its SecureID products in China and is in discussions with authorities there on the development of a national encryption standard.

"We've had some relationships with universities and government in Beijing in developing elliptic curve technology," said Coviello.

This includes a joint venture between encryption pioneer RSA Data Security and Beijing University's Laboratory of information services (Security Dynamics bought RSA in July 1996).

Coviello said the Chinese government has learned from the American experience that controversial concepts such as key escrow and the so-called "clipper chip" often introduce insecurities to the systems that they are meant to protect.

"The Chinese government refuses to buy foreign encryption products because they're afraid that there's a backdoor key," he said.

"This technology is something that governments rightly want to have some control over."

The elliptic curve technology that the company is discussing with Beijing covers key recovery technology, which would enable companies to retain copies of encryption keys generated within their organisations.

Coviello said that government restrictions meant that so far, the company's investment in China had remained "modest."

However, that would all change once a standard could be developed. "We think there's a tremendous market opportunity not only in Hong Kong and

Taiwan, but also in China proper," said Corviello. "It's a market that will be in the tens of millions of dollars in a very short time."

Coviello said that two-factor passwords, such as are used in bank ATM machines, are "the only certain way" to protect confidential or critical data.

Security Dynamics has just released a new family of two-factor password products called SecureSite. The products use one-time passwords that are generated every 60 seconds and authenticated by the same application running on the server.

Argentine hacker pleads guilty

In the first case of a hacker being tracked down with the aid of a court-ordered wiretap, an Argentine hacker has admitted his offences in the US.

Julio Cesar Ardita was accused of breaking into sensitive, but unclassified US government computer networks and returned to the US more than two years after being charged with the crimes.

Ardita, 23, known online as "el griton," Spanish for "screamer," came back to the US voluntarily and pleaded guilty to illegal wiretapping and computer crime felonies. Under the current extradition treaty between the US and Argentina, Ardita could not be extradited.

Under a plea bargain, Ardita agreed to waive extradition and plead guilty to charges he unlawfully intercepted electronic communications over a military computer and damaged files on a second military computer.

The agreement contains a joint sentence recommendation of three years' probation and a \$5,000 fine, US Attorney for Massachusetts Donald Stern said.

According to Stern, Ardita originally hacked his way through Harvard University's computers from his home in Buenos Aires in 1995, accessing NASA and Defence Department computers using stolen university passwords and accounts.

Ardita also was able to hack into computers at the California Institute of Technology, the University of Massachusetts and Northeastern University,

Stern said.

The investigation began in the summer of 1995, Stern said, when the Department of Defence detected intrusions into a number of military and university computer systems containing important and sensitive information about government research on satellites, radiation and energy.

Stern, working with the US Naval Criminal Investigative Service and the FBI, put together an electronic profile of the intruder, using key words such as unique names the intruder gave to files and Internet protocol addresses of systems being targeted by him.

This profile, Stern said, was used to apply for the wiretap order, the first ever obtained to search communications over a computer network, and to configure a monitoring computer to conduct the high-speed searches needed to isolate his activities.

"As this case demonstrates, cyber-criminals know no state or international borders," Barry W. Mawn, special agent in charge of the FBI's Boston Office, said. "Computer intrusions represent a significant crime problem."

"If we aren't vigilant, cyber crime will turn the Internet into the Wild West of the 21st century," US Attorney General Janet Reno said.

"The Justice Department is determined to pursue cyber-criminals at home and abroad."

"This case demonstrates that we will unwaveringly seek to bring international computer criminals to justice," Stern said. "We must make sure that we have a World Wide Web of criminal justice to catch cyber-criminals."

Software myths

Myths surrounding software use are costing firms millions of dollars, according to the Software Publishers Association.

To help debunk some popular urban legends about software use, such as the "24-hour rule" and "abandonware," SPA recently released a policy paper that highlights these two popular myths that Internet software pirates use to justify violations of copyright law.

According to SPA, many software

pirates claim that a "24-hour rule" exists allowing consumers to download or reproduce a program and use it for 24 hours to determine if they want to purchase the software.

Also, pirates declare certain software "abandonware" and regard its copyright protection as outdated. Abandonware is, in theory, a program that has been abandoned by the copyright holder for more than five years because it either lacks distribution or a company's support.

But the unauthorised reproduction or distribution of a program, however, is illegal regardless of the amount of time the software is in use, and like the 24-hour rule, does not exist in copyright law.

"The 24-hour rule and Abandonware are urban legends created and circulated to justify violations of copyright law on the Internet. In fact, neither exists under copyright law," said Joshua Bauchner, SPA manager for Internet piracy and litigation.

"Both the providers of the software and the downloaders, often unsuspecting or unknowledgeable users, may be held liable for this activity," he added.

Industry meets privacy concerns

Growing public concerns over the use of personal information over the Web are giving rise to new initiatives to monitor and control the problem.

A panel discussion presented by the Massachusetts Interactive Media Council heard that groups such as the Platform for Privacy Preferences (P3P), TRUSTe and WebTrust would help introduce new policies and guidelines.

Members of the World Wide Web Consortium (W3C) and Internet Engineering Task Force (IETF) have now completed new technical specifications for P3P, an industry initiative to establish an infrastructure for collection and distribution of information on the Web, said Daniel Jaye, chief technology officer for Engage Technologies.

Meanwhile, TRUSTe, a non-profit organisation formerly known as eTRUST, has finalised stipulations for the TRUSTe seal, to be granted to Web

sites that agree to post specified privacy policies on the use of information gleaned from their sites, according to Russell J. Sapienza, partner, Internet Assurance Services, at Coopers & Lybrand.

A recent survey of Web sites, performed by the group EPIC, found that only 17 per cent are yet displaying any information about their privacy policies, Sapienza told the MIMC audience. Other surveys show increasing concerns among the general public.

Literally hundreds of pieces of proposed legislation on privacy issues are awaiting consideration by the US Congress next fall, he pointed out.

W3C has been working on setting the "social focus" for P3P, and IETF is contributing on the technical side, according to Jaye.

With the widespread collection and dissemination of information about consumers, privacy rights have been subject to infringement for a number of years, Jaye maintained. Ironically, the advent of the Web could help turn things around, he suggested.

"We see the possibility of establishing a privacy infrastructure that 'raises the bar,'" he told the group in Boston.

Engaged is producing user profiles for Engaged-enabled sites, with "guaranteed anonymity" for users, according to Jaye. Users include Lycos and other CMG "sister companies." Microsoft recently purchased Firefly, a major competitor to Engage.

Organisations agreeing to abide by TRUSTe's privacy policies will pay \$300 to \$5,000 per year to be able to display the TRUSTe seal, and will also be monitored to assure compliance.

"Won't this lead to a new breed of class action suits?" asked one audience member, during a Q&A that followed.

Sapienza replied that the TRUSTe seal would meet the criteria of a legal contract. TRUSTe will also revoke licenses of any organisations that abuse the TRUSTe seal by violating terms, according to Coopers & Lybrand.

Other MIMC members vehemently voiced their belief in rights to privacy.

"Our families are (divulging personal information) at the supermarket, in exchange for a couple of discounts," ob-

served one person in the audience.

Marketers today are "selling you for ten cents," asserted another, in reference to the sales of demographic information on consumers between companies.

"It kind of concerns me that the price of a piece of music is higher than the price of information about me," responded a third person.

Speaking at the close of the event, Sapienza said that Coopers & Lybrand has been helping out TRUSTe with "assurance" issues on a pro bono basis.

Coopers & Lybrand has also launched a commercial assurance service, known as WebTrust, that can be hired for Web site audits.

Web site audits can be conducted for a number of reasons, said Coopers & Lybrand's David Kohl, also during the event. Web site operators can use audit reports from Coopers & Lybrand to show advertisers that they are living up to stated statistics regarding numbers of hits, for example, Kohl said.

More information about MIMC is available on the Web <http://www.mimc.org>

Threat of fracking and crypting

Network "cracking" is evolving in a more malicious direction, while adding speciality areas like "fracking" and "crypting" in the process, said members of a new anti-cracking unit.

Staff at Cambridge Technology Partners said that a raft of new words were being coined to encompass the various types of computer system break in.

Really, "cracker" - rather than "hacker" - is the word to use in describing individuals who break into networks, said Wyly Wade of CTP's Enterprise Security Systems Group.

"Hacker" actually refers to anyone who writes program code, even an end user who scripts Microsoft Word macros, Wade said.

Emerging derivatives of the term "cracker" include "fracker," meaning a person who breaks into phone networks, and "crypter," a specialist in cracking cryptographic algorithms, Wade added.

The earliest crackers engaged in the

practice for "humanitarian" reasons, such as the desire to help companies build better products, according to Wade. The humanitarians were joined by those who cracked networks to "further the free exchange of information."

Later on came groups like the PLO, which breaks into networks "purely for profit;" and finally, people whose motives are entirely malicious.

Many of the newest breed of crackers are kids who are unaware of cracking's roots, said Wade, one of eight members of a new anti-cracking Internet security team at CTP.

CTP, a systems integration and software development specialist based in Cambridge, Massachusetts, formed the new group, known as "Core," in response to customer requests. CTP takes a "partnering" stance with its customers, meeting whatever IT requirements need to be addressed, Wade maintained.

With Internet security a rising concern among customers, the new "Core" group stays about a year ahead of the industry at large in keeping on top of new security threats.

The job is challenging, because new "incursions," or security holes, keep showing up every day, according to Wade.

A few of the more popular methods of cracking being discussed at this week's conference include the FTP bounce attack, protocol tunnelling, and tactics such as SYN flooding, which result in "denial of service."

In the FTP bounce attack, crackers manipulate FTP PASV mode, using PORT and QUOTE to send scripts that allow them to gain access to unauthorised FTP servers.

Protocol tunnelling calls for encapsulating, or hiding, one protocol inside of another, such as a telnet inside a ping request.

Many tactics can be used to bring denial of service, including SYN flooding, ghost routing, and service loops, for instance. In this type of attack, users typically do not even realise a server has been hit, instead believing that the server must be busy, or down for maintenance, for example.

Wade pointed out that new viruses continue to fester, as well. Viruses are

already showing up in the 32-bit environment, although some people said this would never happen. And these perennials of cyberspace are certain to land on new 64-bit platforms, as well, Wade predicted.

Cambridge Technology Partners is located at <http://www.ctp.com>

New Thai laws needed

Thailand urgently needs to pass new laws to govern electronic commerce and technology according to a report by the Hong Kong-based New Century Group.

Echoing these sentiments here last week were two partners with Baker & McKenzie, David Shannon and Hatasakdi Na Pombejra, who both pointed out that no law in Thailand yet governs digital signatures.

The report noted that vendors in Thailand regard the lack of laws and regulations as the most significant constraint on the growth of electronic commerce in Thailand.

Laws are currently being drafted by the National Electronic and Computer Technology Centre, which announced at the start of the year that it would push the electronic commerce debate with the government and address the drafts of the related laws.

According to Nectec director Dr Pairash Thajchayapong there will be five draft laws proposed this year. Regulations were being devised by a panel of legal and technical experts from both the private and public sectors.

Later, when the drafts are completed, they will be presented to the National Information Technology Committee for submission to the Cabinet for approval, before being debated in Parliament.

The regulations are said to include a data protection clause, computer crime law, electronic data interchange (EDI), digital signature law, as well as an electronic funds transfer law.

Shannon, who co-ordinates Baker & McKenzie's knowledge base on electronic commerce on a global basis, noted that Malaysia, like Japan, Korea and the United States, had passed laws to cover electronic commerce and computer crime, following recommendations from the United Nations Committee on

International Trade Law.

Other issues are the admissibility of evidence in court, and those relating to so-called "click wrap agreements" where someone agrees to terms on a computer screen by clicking on "I accept," as well as laws to cover computer crime.

Hatasakdi pointed out that existing law could not cover data or data protection, and if this were the case there would be no security for parties offering services, and hence this presents itself as a trade barrier.

AOL boosts security after hack

A vandal who hacked the American Civil Liberties Union site at America Online has caused the giant online service to change procedures to make customer passwords more secure.

AOL only found out who was responsible after the hacker bragged about his identity to a reporter. The firm immediately cancelled the hacker's account, said an AOL spokeswoman, adding that the screen name on the terminated account was PhatEndo.

AOL spokeswoman Ann Brackbill said the hacker called AOL customer service repeatedly, using the name of the person who maintains the ACLU site, to ask for a new password. AOL has clear policies regarding what information is required before a phone representative can make a password change, but the call centres handle 1.5 million calls a week, said Brackbill.

Eventually, one of the firm's 6,000 customer service reps made a mistake and issued the new password.

The hacker went in to post what one report described as "a bizarre one-line message" where the organisation normally posts ACLU-related news.

Brackbill said: "We might have found out about it before the ACLU even did. Apparently we got an immediate call, simultaneously with CNet, bragging about the vandalism."

Asked how the hacker knew the name of the ACLU's site administrator, Brackbill said she was not sure but it might have been by chatting with people in one of the ACLU's chat rooms.

Asked if any legal steps were being taken by AOL against the owner of the hacker's account, Brackbill replied, "We do and always will pursue whatever evidence we have to find hackers but you know they are a difficult group of people to deal with."

"Their names may be fraudulent, for example. But we work very aggressively with law enforcement agencies."

Brackbill said AOL is now routing all password-related calls to a small group of specially trained customer service reps in order to avoid similar problems in the future. The customer rep who issued a new password despite lack of required information was fired, she added.

Need to protect children online

Congress should pass legislation designed to protect children from Internet sex crimes, members of the US House of Representatives were told.

Deborah Boehle told a hearing of the House Judiciary Committee's subcommittee on crime about her own traumatic experience with a paedophile online.

She said: "It was the beginning of a nightmare that no parents should ever have to endure."

"My liberal opinion about freedom of speech literally changed within a split second as my husband read to me the messages that he had found on the Internet that said, in very vulgar terms, that our daughter was having sex with him and that she wanted to have sex with other men."

The messages, and their phone number were posted on 14 different online news groups, such as "erotica.teen" and "luciferslegions," Boehle said, which explained "why we had been receiving phone calls for the past month from men who were asking for our nine-year-old daughter by name."

Boehle said that the messages and phone calls, instigated by their neighbour across the street, were only the beginning of her family's nightmare.

"My husband called the police immediately," she said, and "was told that little could be done."

"The local police said to call the FBI. The FBI said to call the local police. The state police and the state's attorney said they couldn't do anything unless the local police contacted them."

After being advised by the local police to move, Boehle related that in the month before they moved, their daughter "was no longer allowed to walk to friends' houses or ride her bike in the neighbourhood, or even walk out the front door alone."

"We were trying to keep her safe from an enemy that we didn't even know," Boehle said. "A part of her childhood was stolen, and it can never be given back to her."

Boehle urged Congress to pass legislation introduced by Rep. Jerry Weller (R-IL.) that would make it illegal to use the Internet to target an individual under the age of 16 for sexually explicit messages or contacts.

Countering arguments and statements by the Justice Department that laws already exist to protect her daughter, and that Weller's bill could unconstitutionally restrict free speech, Boehle - a city editor at an Illinois newspaper - said "the Constitution was written to protect citizens, not to put us at risk."

"I know there is a price we pay for our freedom, but I do not believe that we should pay with the lives of children," she said. "Freedom of speech is an important and basic right of all Americans, but no one should have the right to put a child's life in danger by abusing that freedom on the Internet."

Weller's bill, HR 2815, the Protecting Children from Internet Predators Act, would amend the federal criminal code to set penalties for using any facility in or affecting interstate commerce, including any computer network or service, to target an individual under age 16 for sexually explicit messages or contacts.

The subcommittee hearing also considered related bills to protect children from online predators, as other members of Congress also urged the subcommittee to approve the bills.

Crime subcommittee Chairman Rep. Bill McCollum (R-Fla.) has introduced legislation that would prohibit contacting a minor over the Internet for the pur-

poses of engaging in illegal sexual activity, and knowingly transferring obscene materials to a minor over the Internet.

HR 3494, the Child Protection and Sexual Predator Punishment Act of 1998, also would authorize pre-trial detention of federal child sex offenders; double the penalties for repeat sex offenders; include a new federal penalty of life in prison for serial rapists; and give law enforcement much-needed tools to track down child abductors and serial killers.

Urging passage of his own bill, Rep. Weller told the subcommittee that "unfortunately, current law does not protect children from these slimeballs who would put their name on the Internet soliciting sexual contacts."

Weller said that although Boehle's situation "may sound like a very unique case ... since Deobrah's story has been in the news, I have been contacted by another constituent who had almost an identical experience. I have been contacted by another mother from Illinois who experienced a similar situation."

US Government to hack its computers

NASA computer experts will try to break into their own systems in an attempt to test security measures.

Last June, NSA agents played a part in a series of virtual war games, code-named "Eligible Receiver," which targeted unclassified computers in the US Defense Department, including the US Pacific Command in Hawaii, to test the system's vulnerability to such attacks.

Eligible Receiver "succeeded beyond its planners' wildest dreams in elevating the awareness of threats to our computer systems," Pentagon spokesman Ken Bacon said.

Bacon said the National Security Agency team also gained access to a US electric power grid.

The computer security tests are part of an overall effort by the federal government to help contain the growing break-in attempts on government computers.

"I think everybody has to realize that we are now entering a period where we

have to worry about defending the homeland again," Deputy Defense Secretary John Hamre said.

"Computer security problems will get a lot worse before they get better," Talleur said, noting the growing sophistication, age and motives behind hacking.

"Many computer hacking cases now involve individuals in their mid-20s to mid-30s," said Thomas Talleur, NASA's Computer Crimes Director.

He added: "They're involved with a number of fringe groups who either perceive the government as the enemy, or are trying to obtain information to destabilize government security."

Computer attacks also are coming from other sources, both inside and outside the government.

Recently an Alabama hacker pled guilty to launching an e-mail bomb attack, damaging transmissions to a NASA electronic mail server system, in violation of the US Computer Fraud and Abuse Act. The court withheld the identity of the juvenile offender, and ordered him to comply with probationary conditions for 12 months.

An investigation by NASA found that the offender launched an e-mail bomb attack last August 4 consisting of 14,000 electronic mail messages across a NASA network against another person using network systems in a commercial domain.

The use of NASA's network bandwidth caused a simultaneous attack against the agency's electronic mail network server at the Marshall Space Flight Center in Huntsville, Alabama, resulting in a loss of network services, Talleur said. Although the juvenile's attack was intended against another individual, and not directly against NASA, other recent cases were more direct.

Recently, a former Kennedy Space Center contractor employee pled guilty in Federal district court at Orlando, Florida, to a charge that he used his workstation to hack into the computers of several Orlando businesses.

"Both government and private industry sources cite the Internet, inside offenders, and certain foreign countries as the biggest threats to the national security of the US."

Product news

Nortel fraud solutions

Nortel has created a new Fraud Solutions division that aims to offer wireline and cellular telecommunications operators a range of security hardware and software.

To launch the new operation, the UK company has launched SuperSleuth, a neural network-based fraud detection package for telecom network operators, whether wireline or wireless.

Bill Seymour, the new division's general manager, said SuperSleuth is a next-generation package that can run on a variety of telecoms platforms, including Unix, and is able to analyse and adapt to new fraud patterns as they occur.

According to Seymour, the SuperSleuth system combines state-of-the-art neural network-based technologies with more traditional rules-based detection to provide a "comprehensive" telecom fraud software system.

"The neural network side of the software is the most advanced in the business," he said, adding that the software can spot unusual activity on a user's account, whether it is a hard-wired phone or a mobile phone.

"Fraud is now all pervasive in the field of telecommunications, and the integration of fixed with wireless services mean that many companies are worried about their exposure to fraud," he said.

According to Seymour, unlike earlier packages, the SuperSleuth system's adaptive neural network technology does not require operators to set specific thresholds for a group of users, such as the number of international calls made in a particular time period, or the value and duration of calls, and does not need to be reprogrammed to recognise new fraud patterns.

As a result, the company claims, it is much more effective in keeping up with fraudsters' techniques, which Nortel estimates currently cost operators around the world £13 (US\$22) billion a year.

Seymour says that SuperSleuth is "a major breakthrough" in the fight against fraud.

"Because neural networks learn quickly and are adaptive, they are highly effective at identifying fraud in situations where calling patterns change rapidly,

such as in the cellular industry," he said, adding that the system works by scanning customer data records in near real time and alerting fraud analysts when it detects calling patterns which may be fraudulent.

According to Seymour, as human operators confirm incidences of fraud which the SuperSleuth system has recognised, it continues to learn.

Accuracy, he said, improves as the neural network matures, so cutting down wasted time on false alarms.

One interesting feature of the SuperSleuth software is that it can also handle huge quantities of data, and provides network operators with individual calling profiles for individual subscribers.

"This will significantly increase the productivity of fraud analysts," Seymour said, adding that the SuperSleuth system has been measured to raise up to 20 times fewer false alarms than competitive fraud detection products - so saving network operators both time and money.

According to Seymour, Nortel Fraud Solutions is developing a whole family of complimentary products designed to help operators gain a better understanding of the behaviour of their customers.

Nortel's Web site is at www.nortel.com.

New 32-bit Disknet technology

Reflex Magnetix has unveiled two new 32-bit versions of its Disknet Data Security suite.

According to the UK firm, these latest versions of Disknet Data Security are designed for easy deployment throughout Windows NT and/or Windows 95 environments within organisations that need the highest levels of information security.

Officials said that the software provides the most effective protection yet for networks of Windows PCs - not only from external threats such as hackers and viruses, but from careless or disgruntled "insiders" as well.

The company says that, unobtrusively but firmly, the Disknet Data Security suite forces every user on the net-

work to scan for viruses - it prevents tampering with PC configurations, and eliminates the risk of copyright breaches by stopping users loading unauthorised software.

Additionally, Reflex says that the NT version can secure the organisation's sensitive data with an automatically encrypted hard disk of up to 4.0 gigabytes in size.

According to the firm, the new 32-bit releases of Disknet Data Security are the first to be supplied to Reflex's non-military customers in two distinct versions: the Administrator and the Client.

The Administrator is said to be intended for use at the server (or on a minimal number of management workstations). This leaves the lower cost Client version to be deployed on the remaining network PCs.

The Disknet Data Security Administrator is supplied complete with Sherlock, which is billed as a fast 32-bit virus scanner based on the ThunderByte engine. Reflex Macro Interceptor, a dedicated macro virus scanner, is also provided.

Reflex recommends that, for additional assurance, its customers add at least one further third party Windows 95 and NT scanner alongside Sherlock and Macro Interceptor.

Most popular AV scanners are supported, including Dr. Solomon's Anti-Virus Toolkit, F-Prot, VET, Norton AntiVirus, and McAfee VirusScan. The firm says that up to four different scanners can be deployed in a Disknet-protected environment at any one time.

According to Reflex, the Disknet Data Security Client can be installed and upgraded (if necessary) over the network, enabling IT managers to deploy the program in a very cost-effective manner and with "minimal disruption" to users.

To help achieve better overall control of network security, the administrator can be set up to create a configurable audit log on the server of any virus incidents and/or attempts at unauthorised operations.

Further details of the new package can be found on the company's Web site at <http://www.reflex-magnetix.co.uk>

Hardwall security

Vircon, a division of Calluna Technology, has launched Hardwall, a hard disk partitioning system designed to protect data.

According to the company, Hardwall is a radical new approach to computer data security. The system, which sells for £185 per site license, is billed as protecting data held on a server's hard disk by the intelligent use of disk partitioning.

Sue Starie, a spokesperson for the firm said that the system is well suited to applications involving networks, such as the Internet.

As well as using intelligent disk partitioning, the package is said to provide protection against virus attack, hacking, data theft, illegal access, as well as data corruption and has been designed to meet a user's specific data security requirements.

Hardwall is supplied on a printed circuit board plus driver software and is said to be installable by even computer novices.

The firmware on the PCB drives a microprocessor that operates independently of the host PC's processor. The PCB slots into a standard ISA card slot on a PC chassis and connects between the hard disk drive and the motherboard of the PC.

While installing the system, users can decide what data to store in each partition and define access rights to these partitions, dependent on the level of protection required and the type of data stored.

Hardwall then sets up "hard firewalls" at the partition boundaries - at the start of the session, the user selects a partition, which becomes "active" and Hardwall then ensures that the protection rights assigned to each nonselected partition are obeyed, so preventing illegal accesses beyond the partition boundaries.

Unlike other security devices, Hardwall is not virus specific and, as a result of this, the firm says it can ensure system integrity at all times.

The Hardwall card and software is available immediately and is said to be compliant with Windows 3.xx, 95, and NT operating systems.

Peter Barlow, Vircon's general manager, said that there are over 16,000 known computer viruses and that number grows every day.

"As more and more computers are hooked up to the Internet and other networks, security is becoming a real issue for every computer user," he said, adding that Hardwall is a unique hardware approach to overcoming the enormous combined threats of virus attack, hacking and the corruption of system configurations, which face companies and home users alike.

"So far, all tests indicate that Hardwall is the foolproof solution we've all be waiting for," he said.

Cures for first PowerMac worm

Two firms have announced cures for the worm virus which affects Macintosh computers and can cause poor performance and even data loss.

Dr Solomon's Software has launched a Virex Virus update to cure the new AutoStart 9805 worm and Symantec Corp has posted its own cure on the Internet.

The AutoStart 9805 is the first known worm capable of infecting Apple Computer Macintosh PowerPC-based machines.

The intentionally destructive worm is selective. AutoStart 9805 does not affect non-PowerPC Macintosh systems, those with 680x0 processors, and even a Power Mac must be running QuickTime and an active CD-ROM AutoPlay feature to be affected.

AutoStart 9805 is transmitted via HFS or HFS+ Macintosh-formatted disk volumes, meaning just about every type of disk including floppy disks, most removable cartridge drives, hard disks and disk images.

Dr Solomon's said the worm got its start in Hong Kong and has spread rapidly throughout the world.

A worm, unlike a virus, replicates itself from one computer to another as a self-contained, stand-alone file, instead of infecting programs or documents.

When spreading, the AutoStart 9805 worm is seeded as a hidden AutoStart

application file called "DB" in the root directory of any mounted volume.

The worm does its damage when QuickTime's CD-ROM Auto-Play feature, which launches an application or document automatically when a disk volume is mounted, is active. Disk activity and, if mounted, network activity, increase drastically, and so performance problems may be the first symptom noticed.

As another early symptom of infection, the system may unexpectedly restart after mounting a disk or other volume. This happens only when the worm is first introduced, said Dr Solomon's.

Symantec said the worm's DB application tries to transform itself into a hidden system extensions file called "Desktop Print Spooler."

About every 30 minutes, Desktop Print Spooler searches all mounted volumes for an extensions folder to continue propagating itself. This search is what degrades performance. Once the worm is active, the "DB" application name will flash briefly in the menu bar when a new disk is mounted.

After searching all mounted volumes, AutoStart 9805 begins checking for files ending in .dat, .cod, .csa, and .data, and tries to overwrite them with random data.

When it succeeds, the corrupted files are irreparable and must be reinstalled or restored from backups.

"AutoStart 9805 is the first real Macintosh virus threat in three years and a very dangerous one at that," stated Jan Sutton, worldwide product manager for Dr. Solomon's Virex.

Users of Dr Solomon's antivirus software for the Macintosh can find Virex Virus Update 05-02-98 and later, which detects and removes the AutoStart 9805 worm, on the World Wide Web at <http://www.drsolomon.com/products/virex>.

Users of Symantec AntiVirus for Macintosh 4.5 or Norton AntiVirus for NetWare users can download the worm definition update from Symantec's bulletin board system, via File Transfer Protocol, or Web site or from Symantec's forums on CompuServe and AOL.

The Symantec Web site is at <http://www.symantec.com>

NAI to buy Secure Networks

Network Associates Inc. has agreed to buy Secure Networks Inc., publisher of Ballista, a network security scanning tool that does what might be called "ethical assaults" on networks.

The program uses various tricks to penetrate a corporate firewall and commit other simulated mischief, then issues a report on whatever weaknesses it finds. It's a robotic equivalent of the "friendly hacker."

As the NAI source sees it, Ballista completes NAI's assembly of a network security toolkit that can now be considered truly "end to end," as NAI publicity types like to label it.

NAI has been assembling the suite for quite a while. The firm wants its security toolkit to replace stand-alone network security tools much the way MS Office replaced stand-alone spreadsheets, word processors and the rest of the Office collection of programs.

NAI said: "With Ballista, the NAI suite does everything needed to secure a network against marauding hackers, viruses and other threats - at least until we reach the next stage of the continuing hacker war."

NAI itself was formed from the marriage last year of McAfee Associates and Network General Inc. in a widely reported merger.

Since then, NAI has digested both Pretty Good Privacy, the public key encryption firm, and Trusted Information Systems.

NAI now claims to be the only network security firm able to offer the gamut from firewalls and global VPNs (virtual private networks) to intrusion detection, audit analysis, encryption, authentication, anti-virus and - with Ballista - security scanning program.

NAI maintains a Web site at <http://www.nai.com>

Cyber data insurance to protect Internet

Computer giant IBM has started to work with insurance firms to look at new

policies which cover the hazards of using the Internet.

IBM's Lynne Brown, speaking at the Summit '98 conference in San Francisco, warned: "The information highway runs right up to your door."

As the Internet continues to hurl forward, spaces once tucked away in the relative safety of "private" back roads are quickly becoming easy prey for highway hijackers, hackers, vandals, and conmen.

"DNS (domain name server) hijackers" are using spoofing to steal the identities and good names of corporations and their World Wide Web sites.

Pinging and smerfing also run rampant. And at last count, there were 440 sites on the Web dedicated to the crime of hacking, according to Brown.

The US national predilection to levying lawsuits is also catching up with the Internet. People who run Web sites need to be wary even of "errors and omissions." In one actual case, a bed and breakfast in Hilton Head, South Carolina posted a weekly room rate of \$600 on its site, she illustrated.

The rate subsequently rose, but the site was not updated. A Web surfer who called the B&B by phone was quoted a price of \$1,200, and then proceeded to sue.

IBM is already working with a number of insurance companies on "data insurance," including Cigna International; Reliance; and NRMS, the Summit audience was told.

Various kinds of policies are now being explored and developed, such as: product liability; carriers' and providers' policies; and even policies for "officers and directors", who could also be held liable for an organisation's misdeeds or mistakes in cyberspace.

IBM is on the Web at <http://www.ibm.com>

Voice "fingerprints" to cut fraud

Cellular cloners in Pittsburgh in the US should beware, as AT&T Wireless Services has installed a Corsair PhonePrint RF fingerprinting system.

Officials say that the deployment of the anti-cloning technology follows on

from installations in other AT&T Wireless markets, including New York-New Jersey, Las Vegas, Santa Barbara, and Oxnard-Ventura.

The PhonePrint system works by logging the RF fingerprint of a given mobile and comparing it to further call requests made by a given ESN/MIN (electronic serial number/mobile identification number) pair, which all analogue mobile numbers present to the network to ID themselves when logging on or placing a call.

Skip McDowell, Corsair's vice president of sales, said that the Pittsburgh deployment helps to round out an increasingly comprehensive PhonePrint presence in the region.

"Our PhonePrint Roaming Network makes it much more difficult for cloners to turn to roaming fraud as an alternative to cloning in their home markets," he said.

"This aspect of the system becomes more effective as more markets install PhonePrint, and we now have an extensive system in much of North America.

The practical effect in many markets is to force cloners off the wireless system altogether," he explained.

For more information contact Corsair Communications on +1 650 842-3263

Putting criminals in the picture

Software firm Visionics says its FaceIt7 PC software system is now available for regular PC users for a variety of security uses.

FaceIt7 PC is based on the FaceIt DB heavyweight security system for high-power enterprise users.

A Visionics spokesperson said the system "captures your image as you walk through an office building, department store or airport.

"It immediately links your image up to a database that reports back to local security if you are wanted for a crime, or are a missing person."

The Visionics spokesperson said the new PC version lets workers or home users leave their computers without concern about privacy issues or intruders.

The program automatically secures

the system with a screen lock and only unlocks when the authorised user shows his face again - literally. There is no need to enter keystrokes since the program automatically recognises a user.

FaceIt PC also records all persons who come into an area, whether they want their picture taken or not.

The program can then forward the images to a remote system, if told to do so. This lets a user keep track of what is happening at an office or at home.

A mini-movie greeting left on a machine can invite visitors to leave a text message along with the facial image for authorised users to retrieve later, or send to a remote location.

Its makers say FaceIt's encryption software protects confidential files, then uses facial identity to unlock the decryption program.

The spokesperson said the PC version of the program is based on the US data encryption standard, or DES.

FaceIt PC requires a 90 MHz or faster Pentium system with Microsoft Windows 95, a CD-ROM, a Microsoft Video for Windows-compatible video capture system with 320x240 resolution and 15-bit RGB capture-to-memory of five frames per second.

Visionics Web site is at <http://www.faceit.com>.

Ontrack adds virus finder

Data recovery firm Ontrack has added a virus scanner to its Data Advisor diagnostic package to help fix computer problems.

The software, which operates even when a computer is unable to boot, now allows users to pinpoint viruses as well as PC hardware and software problems.

Richard Keech, general manager of Ontrack UK, said: "Currently PC users need two products - a disk diagnostic tool and a virus checker - to identify the most common problems that might occur on their computers.

"Data Advisor combines the best of both functions, making it an invaluable product in case of an emergency."

For more information visit the firm's Web site at <http://www.ontrack.com>

Password protected e-mail unsecure

More than one in ten e-mail messages from Fortune 1000 companies in the US are being read by someone other than intended recipients.

A US Senate survey found 12.6 per cent of Fortune 1000 companies reported evidence of e-mail tampering. However Cyber-security specialists RPK says it believes the actual incidence among the 200 million e-mail messages sent per day is dramatically higher.

It said that transmitted password protected files can be read by anyone with basic computer techniques typically used by hackers.

Lawyers and accountants topped a list of most-likely targets for e-mail tampering, but they were followed closely by banking and financial professionals, management consultants, military contractors, and importers and exporters.

A third of e-mail privacy problems involve corporate eavesdropping. E-mail privacy experts who developed Pretty Good Privacy (PGP), a free e-mail encryption program, cite a survey which shows as many as 25 per cent of companies eavesdrop on employees' mail.

RPK spokesperson Lyn Oswald said: "Once you send e-mail from your desktop, you are sending it through a number of servers. Anywhere along those servers, hackers and employees can tamper with your e-mail."

The answer, according to RPK and other experts, already exists, but companies and individuals are not taking advantage of existing technologies.

RPK says that encryption and authentication technologies are available, but products which incorporate these technologies require senders and receivers to have the same security software to code and decode messages.

"This means every person who receives an encrypted e-mail must have a corresponding software to remove the encryption."

RPK's InvisiMail, a \$29.95 software product, allows users to authenticate and encrypt e-mail.

"You definitely want to encrypt sensitive data," continued Oswald, "but it is

easier to encrypt an entire message to make sure you are completely protected."

Experts believe businesses and individual desktop computer users should take the time to encrypt e-mail messages, but the issue is similar to backing-up computer data. It is only an issue after disaster strikes.

More information is available at RPK's World Wide Web site at <http://www.InvisiMail.com> or at <http://www.vservers.com> for PGP.

Strong encryption for Japan gets go ahead

Hewlett Packard has announced it has received approval from the US government to export its strongest encryption system to Japan.

The approval means HP's VerSecure technology, which utilizes 128-bit and triple-DES encryption, is now available to customers in Japan.

Users can choose from limited to very strong cryptography and select whether or not to use key recovery capability. An unannounced security domain authority, a trusted third party, will install and manage the VerSecure system in Japan.

It will be responsible for making encryption policy that adheres to Japanese law and will distribute software tokens that activate encryption capabilities that support Japanese policy for Japanese companies, said HP.

Other nations that HP has received United States government clearance to export the system to are the UK, Germany, France, Denmark and Australia.

"Japanese companies represent some of the world's biggest players in today's electronic world, so secure communications and transactions are essential," said Lewis E. Platt, HP chairman, president and chief executive officer.

"VerSecure has hit the ground running in other countries, and we know that this innovative technology will provide Japanese businesses and consumers with the peace of mind and freedom-of-choice to exploit the full power of the Internet and to conduct an array of electronic transactions — all the while balancing concerns about fraud and privacy."

CompuServe trial

In a surprise move, the former head of Internet service provider CompuServe in Germany has been convicted of distributing pornography. Paul Johnson looks at the case surrounding Felix Somm and the implications for the future.

Few industry insiders thought he should have stood trial, never mind actually be convicted. But Felix Somm was found guilty and held personally responsible for allowing CompuServe Deutschland customers access to undesirable sites, even though prosecutors changed their mind in the case.

The state has alleged that Somm should be held responsible for the company's actions in allowing open access to the Usenet, which contains images and other files relating to the Nazi party and illegal pornography.

Ironically, although Somm, 34, was accused almost three years ago by the regional legislature, he left the company last summer to form his own consulting firm.

The case looks likely to propel Somm from a humble, but experienced, Internet consultant, to something of a celebrity in the German online scene.

Somm said he expects to be cleared of the charges. In a statement, he said that he is convinced that this appeal will prove his innocence.

"The charges are based on a misunderstanding of the structure of the Internet and the role of service providers," he said, noting that he also assisted the German authorities with their investigation once it became clear that there was a problem.

The Bavarian government accused CompuServe Deutschland of breaking the law by allowing German online users access to illegal material on the Internet in 1995. The move resulted in CompuServe having to "regionalise" its access facilities to ensure its ability to meet local country requirements.

Despite the move, Somm was charged with various offences under German legislation in March of last year, a move which upset civil liberties groups both in Germany and in other countries to the extent that they have banded together to lobby the German government over the affair.

In late March of last year, a coalition of civil liberties organisations from

a dozen countries wrote to the German Chancellor, Helmut Kohl, to express their concern about Somm's prosecution.

The letter stated the prosecution of Somm was "ill-advised for both technical and regulatory reasons" and will "have a harmful impact on Internet users around the world."

The organisations signing the letter, initiated by the Global Internet Liberty Campaign, include the American Civil Liberties Union, Arge Daten, Association des Utilisateurs d'Internet, Derechos Human Rights, the Electronic Frontier Foundation, Human Rights Watch, the Internet Society, and Privacy International.

CompuServe Deutschland supported Somm in his defence, and enlisted the assistance of Ulrich Sieber, a respected university professor and an expert on IT

legislation.

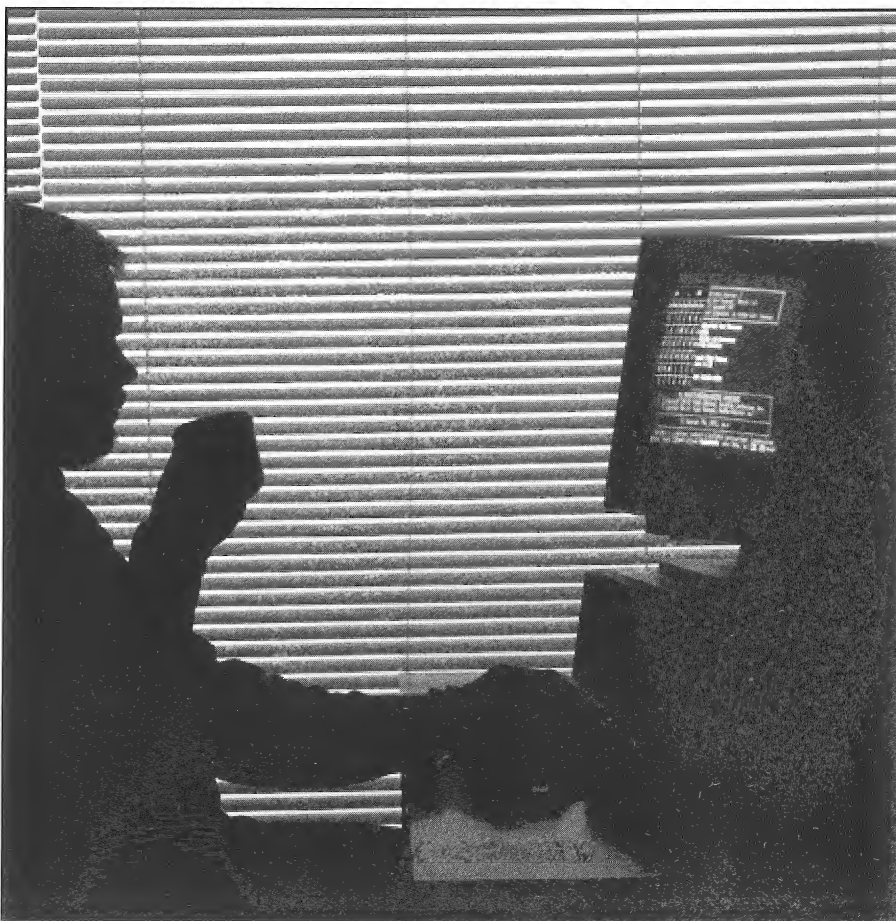
According to Sieber, the new legislation, known as the Multimedia Law, that kicked in last summer, made it clear that an individual could not be held responsible for the content of the Internet.

"The accused is not the originator of the illegal data, and intensively supported the Bavarian police in tracking down the originators," he said.

Under Germany's Information and Communications Law, which came into force last August, Internet access and service providers are not held responsible for banned material on the Internet, providing they were unaware of the existence of the material. This was the first conviction under the new law.

Somm's lawyers said that since the problem first came to light, CompuServe has worked hard to solve the problem in Germany and also provides subscribers with special software that blocks access to illegal and offensive material.

The ISP giant axed 200 electronic message boards for all of its then four million users worldwide, setting off an



international debate over censorship on the Internet. But in February 1996, the firm reinstated all but five of the boards and introduced software to allow customers to block unwanted material.

Prosecutors in the *Somm* trial even argued for his acquittal in a dramatic about turn after they said it was unreasonable to have expected him to block illegal material with the technology that was available in 1995 and 1996, the time when charges were brought.

In the prosecution's closing argument, lawyers said they still opposed the view that online service providers had no responsibility for outside content in all cases, but added that there was not enough evidence to show that *Somm* intended to distribute pornography.

But even with the prosecution's U-turn, the Munich district court convicted *Somm* of complicity on 13 counts of spreading banned pornography on the Internet and gave him two years suspended sentence and ordered him to pay DM 100,000 (\$57,500).

The judges agreed with the Bavarian prosecutor's original position because *Somm*, as CompuServe's senior executive in Germany, provided Internet services that made the materials accessible to Bavarian subscribers of CompuServe.

"Even on the Internet, there can be no law-free zones," the court said in its verdict. "The accused is not a victim. He abused the medium."

Judge Wilhelm Hubbert said CompuServe had let "protecting the young ... take second place to maximising profits," adding that he wanted the verdict to deter other Internet-access providers from doing the same.

Defence attorney Wolfgang Dingfelder called the verdict "complete rubbish" and promised an appeal.

According to *Somm*'s lawyer, Hans-Werner Moritz, the court failed to give weight to statements of experts, the revised position of the prosecution and German law regarding multimedia. "Certainly the fight will go on," he said.

The new Information and Communications Law declared that Internet service providers are not generally held liable for material on the global Internet. They are required to take reasonable measures to block access to banned ma-



terial, however.

Appeal

In a surprising move, the court decision has been appealed by both the prosecution and the defence.

Defence attorney Hans-Werner Moritz said he was confident the prosecution's unusual move for reversal would help to clear his client.

"We are very confident and we very heartily welcome this motion by the prosecutor," Moritz said.

"I think the decision will be overturned. It has to be. The judge put forward a decision that is completely wrong."

He said that the prosecution's appeal was separate from the defence effort but added weight in *Somm*'s favour.

The prosecutors' appeal reiterates their new position that technology to block banned material on the Internet was not available in 1996.

The appeal process cannot go forward until Judge Hubbert submits a written decision.

After that, Moritz can appeal to the district court, where he can argue for a reversal based on both Hubbert's reading of the law and the facts in the case.

An appeal to the Bavarian superior court could be argued only on legal grounds, he said.

"We haven't decided which way we

will go but it will probably be the superior court," Moritz said, noting that under the multimedia law the case should not have come to trial.

"The court completely overlooked the law," he said, adding that prosecutors made a move for acquittal based on the powers of the multimedia law. "It's completely out of the ordinary."

Prosecutor Manfred Wick said his office needed to review the judge's written opinion before deciding whether they would challenge the verdict on points of law or seek a new trial.

He said the appeal is being made independent from defence efforts to have the verdict overturned. "But we're striving for the same result," he said.

Reaction to the case

Politicians, officials and industry leaders have been surprised by the court result, and fear it could result in the Internet being stifled in Germany.

The German government said it would examine the court's decision carefully. "The development of the Internet in Germany must not be held back. This is about the jobs of the future," declared Technology Minister Juergen Ruettgens in a statement.

Germany has not recovered from recession and the impact of reunification with East Germany. Any development that could effect the job market or trade will come under close government scrutiny.

Joerg Tauss, a federal lawmaker from the opposition Social Democrats who specialises in multimedia issues, called the result "a catastrophe" that would "ruin the Internet in Germany."

He said: "The Justice Ministry had said, absurdly, that it would demand tougher laws if there was an acquittal."

"We can only assume that the judge, who was clearly Internet-illiterate, was egged on by the ministry."

A Bavarian Justice Ministry spokes-

man said his department could by law make no comment on the outcome of the trial.

Christopher Kuner, a Frankfurt attorney representing several multimedia firms, said it might make some reconsider doing business in Germany. "It's going to create a sort of chilling climate in terms of new investment," he said.

Even prosecutor Franz von Hunoltstein said the decision would have "very clear economic effects."

Kuner said the verdict showed that Germany's wide-ranging multimedia law, which government officials said would provide a boost to the industry when it was passed last year, was still too vague.

"The law was touted as removing the possibility for this happening," Kuner said. "This is going to have a very bad effect."

Kossel also voiced concerns about the decision's implications. "If it stands, it will strongly slow down the development of Internet technology in Germany and use of the Internet for business," he said. Small Internet providers would likely face higher costs to block materials on the Internet and might pull out of Germany, he said.

Larger companies would have to weigh the risk of further lawsuits and the cost of blocking material located on computers in other countries.

Steve Case, chairman and chief executive officer of America Online Inc., which now owns CompuServe, called the conviction "outrageous" and US presidential advisor Ira Magaziner said he "wouldn't be surprised if the conviction is overturned."

An AOL spokeswoman said the firm was "surprised and disappointed" by the verdict, which it said "appears to reflect a fundamental misunderstanding of the unique characteristics of the Internet and the role of Internet providers."

European Union says ruling contradicts law

European Commission officials said that they found the conviction of Somm on pornography and indecency charges "surprising."

Somm sure verdict will be overturned

Felix Somm said that he is "100 percent confident" that the court decision will be overturned.

Somm also said the ruling was wrong and felt that it could set a dangerous precedent for the development of the Internet in Germany.

He said: "The prosecutors in the end agreed with us. All the experts supported us. (The decision) is not in accord with the law."

Somm, a Swiss, said support has swelled since the decision reverberated throughout cyberspace. He has received scores of e-mail messages from around the world, while an online petition has been set up to collect signatures calling for a reversal. "I feel pretty good about that," he said.

At the same time, Somm said the case has been a burden to him and his family since the charges emerged in April 1997. "It has been very hard

for me and for my parents to see my name connected with something like child pornography," he said.

It has also weighed on his new company, Somm.com, an electronic commerce consulting firm, which he started after leaving CompuServe in July 1997.

If the ruling stands, Somm said other on-line providers or e-commerce companies could be hurt as well, as many experts have said.

"All providers must be concerned and nervous to see what happens," Somm said.

"The chances for the next step are certainly better and more convincing if the prosecutor and defence make the same motion - for acquittal."

"Naturally we are going forward with our legal action, but I am very thankful for the clear and sincere line of the prosecutor," Somm said.

A commission spokesman said that the EC "learned of this decision with a certain astonishment," and that the ruling seemed to contradict German law.

The carrying of information across international borders needs to be addressed, Commission spokesman Jochen Kubosch said, and should be coordinated among countries.

"This proves once again the need for talks at international level about this type of problem," he added.

The European Union executive has been pushing countries to adopt an international charter setting out procedures for addressing legal and technical questions affecting the Internet and other electronic networks.

Kubosch said liability for information carried across borders on the Internet needed to be addressed.

"The legislation on this subject, when it exists, is different in the different countries of the world," he said. "So it would be very useful to co-ordinate a little and should be one of the subjects covered by the charter."

The Commission has promised to propose EU legislation this year on the

liability of on-line service providers for content carried over their networks in areas such as obscenity, defamation, privacy and misleading advertising.

But the EU so far has promoted industry self-regulation and filtering technology as the best way to control Net content that is illegal or harmful to children.

EU telecommunications ministers agreed recently to fund a four-year action plan to cover initiatives such as a European network of hot lines to allow users to report illegal material.

Net groups' verdict

Internet groups feared the CompuServe verdict would be seen as imposing liability on online service providers for every message or posting carried on their systems.

"An international company, CompuServe, has had its employees subject to the criminal laws of Germany," said Barry Steinhardt, president of the Electronic Frontier Foundation.

"There will be a fear among many Internet service providers of doing busi-

ness there and a fear that they're going to be subjected to a variety of national laws."

Steinhardt said an international agreement was needed to limit the liability of service providers. Germany itself enacted such a law, called the Information and Communications Law, but not until after Somm was charged.

"Even if there's an appeal, there's a significant precedent being set here," said Jerry Berman, executive director of the Centre for Democracy and Technology in Washington. "It is a great setback for a decentralised, open communications medium."

Berman said the real answer to Internet pornography was "empowering users" by making available software for filtering out objectionable content.

Germany's leading Internet service providers said they see their continued operation in Germany threatened by Somm's conviction.

Germany.net and Deutsche

Telekom's T-Online as well as CompuServe and its parent company AOL said in a joint news release the case was a legal setback that created confusion over their legal liabilities.

The four Internet service providers said the decision "puts in question the decision of whether to operate an online service in Germany or to provide access to the Internet."

They said providers who only create technical access to the Internet must not be held responsible for illegal content or else growth in the industry will be choked off, with serious consequences for Germany.

They condemned the dissemination of illegal material via the Internet and said they supported efforts to apprehend those who posted it.

But they said the Somm decision made Internet service providers into scapegoats and made no constructive contribution toward eliminating the problem.

Bavarian cybercops hunt online criminals

Germany has several other unique laws that are at variance with the freedom of speech and the press in other leading Internet jurisdictions such as the US.

For instance, it is a crime in Germany to deny the Holocaust or to disseminate Nazi materials.

The court sits in the capital of Bavaria, widely seen as the most conservative of Germany's 16 states. The large southern state, centre of the country's hi-tech industry, launched its crusade three years ago after deciding the global computer network was running out of control.

Bavarian police have a special unit staffed by six officers, set up in 1995, that trawls the Internet for pornography involving children or violence and Nazi literature.

But the Bavarian cyber police's efforts to secure convictions have often been thwarted because material passed on to other countries is not always acted on by those police forces.

Their job is also subject to the normal constraints of how undercover police officers are allowed to operate. The police can, for example, hang around electronic "chat rooms" where computer users trade information and swap material.

But they cannot incite anyone to commit a crime, hoping instead the users offer illegal material of their own accord. The mere threat of conviction might, however, be having the desired effect in encouraging Internet service providers to look at new ways to limit access to material.

"There has been a huge discussion of this issue among service providers in the region," said Harald Summa, business manager of Eco Electronic Commerce Forum, a grouping of German businesses seeking to promote the Internet.

"Some are now putting in place voluntary measures of their own," he added.



UK encryption policy

The British government unveiled its policy on data encryption which mixes voluntary registrations and new search and seizure legislation.

Earlier reports had suggested that the British government was looking to the key escrow system favoured by the Clinton administration in the US.

Announcing the proposals, UK Trade Minister Barbara Roche said the government would set up a voluntary registration scheme for those using strong cryptography. Legislation would also be introduced that would give police the right to ask a court for a warrant to search computer files instead of buildings.

The plan is to create a number of trusted third parties (TTPs) which will be able to register their encryption keys. These TTPs, she said, will in turn be licensed by the Government to ensure public confidence.

According to Roche, encryption is essential to the future of Internet shopping and electronic commerce, but also provides criminals and terrorists with the opportunity to disguise their activities.

As a safeguard, the government proposes to change the law so that police or other civil authorities can request a search warrant, making the possibility of evasion unlikely. One other proposal under active discussion is to create a new family of certified authorities to guarantee digital signatures.

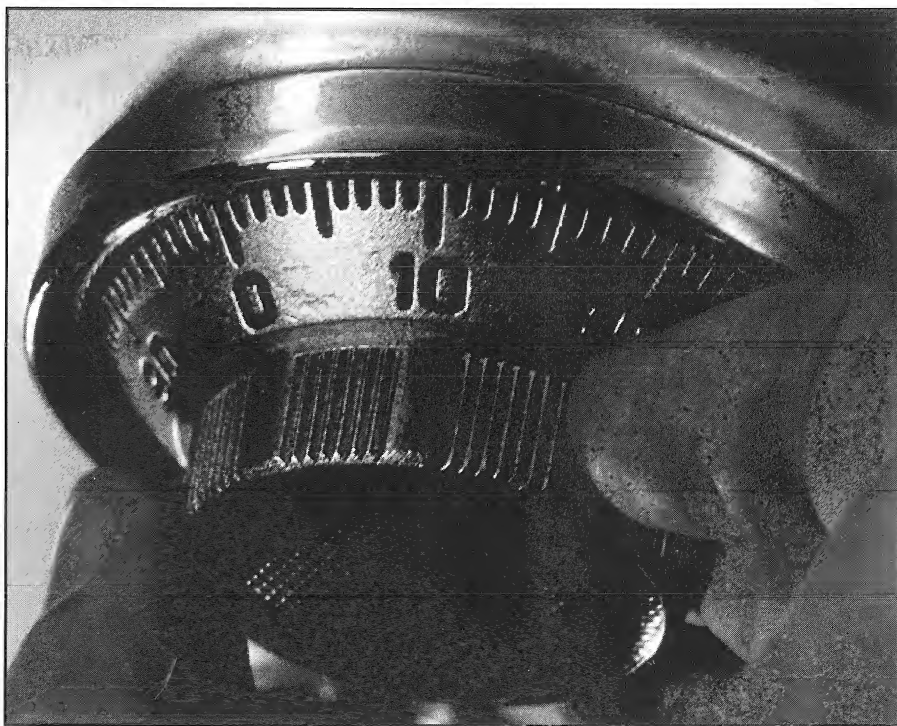
Roche said that it is important to make electronic commerce more secure.

"Users cannot afford to let the information they transmit across the Internet, or any other network, be compromised," she said, adding that they must be able to trust both the technologies which allow such security and the commercial organisations providing it.

Plans call for accredited experts to be known as C:Cure experts.

According to Roche, the C:Cure standard will allow companies of all sizes to demonstrate the effectiveness of their IT security systems to prospective trading partners.

"It also enables firms to benchmark their arrangements against accepted best practice - I hope that C:Cure will enable more British businesses to reap the competitive advantages which electronic trading can bring," she said.



The government's plans for encryption are based on an ongoing consultation process that has been going on for several months. Last year, the Department of Trade & Industry issued a consultation paper that requested further input into the use of trusted third parties for encryption.

That paper, officials said, brought 260 responses. According to the DTI, some were based on apparent misconceptions, and only a few approved the proposals without qualification. According to the DTI, most approved the idea of licensing TTPs.

One well-known encryption expert, Dr Ross Anderson of Cambridge University, said that Roche's proposals were a sudden about-turn from Labour's pre-election promises.

Creating licensed TTPs, he said, would put great pressure on the public to use them whether they wished to or not, and was rather like introducing a voluntary identity card scheme.

"The thing about voluntary identity cards is that eventually they usually become mandatory," he said.

"I regard this as a U-turn from Labour. In their manifesto they led us to believe that they would avoid this path, but in fact they have followed almost exactly the previous Conservative government's

policy," he said.

"Instead, they should have left well alone and waited for a degree of consensus internationally. Under their present proposals, my electronic signature could be perfectly valid here and not in Germany," he said.

Roche, meanwhile, said that there are plans to develop the TTP on an international basis. Interest, she explained, has already been expressed in the new standard as applicable for Europe, the US, and Australasia.

"The use of suitably qualified independent auditors and the close involvement of end users are just as critical to international success," she said, adding that "it is vital that companies have the high degree of confidence which only these features can give."

"Information security is primarily about people and how they use technology. C:Cure cannot, therefore, be an absolute guarantee - but it does show that organisations under it are committed to information security," she said.

According to Roche, it also shows that they have looked at best practice in the light of their business needs. She said: "it demonstrates that they have given serious consideration to all the security threats they face, and that they have appropriate safeguards in place."

DIVA - computer evidence

Digital Integrity Verification and Authentication

It is a basic axiom that an effective encryption/verification system should retain its security even if the "enemy" has the mechanism and the technology to use it.

Here Jim Bates, from Computer Forensics Ltd, presents an overview of the subject and looks at one way forward in this important area.

As police officers and other investigators become more familiar with handling evidential computer material it is apparent that a number of more or less formalised procedures have evolved to maintain both the continuity and the integrity of the material to be investigated.

While these procedures are extremely effective under the current UK rules of evidence, it is expected that alternative procedures will develop as technology advances.

The current procedures in use by both Police and civilian users of the DIBS® system in the UK work something like this:

At least two copies are taken of the evidential computer. One of these is sealed in the presence of the computer owner and then placed in secure storage. This is the MASTER copy and it will only be opened for examination under instruction from the Court in the event of a challenge to the evidence presented after forensic analysis on the second copy.

If the computer itself has been seized and held in secure storage by the Police, this will constitute "best evidence". If the computer has not been seized then the MASTER copy becomes best evidence.

In either case, the assumption is that whilst in secure storage there can be no possibility of tampering with the evidence.

This does not protect the computer owner from the possibility that secured evidence may be tampered with.

A growing practical problem with this method of evidential copying occurs not with the security aspect but because of the increasing sizes of fixed disks found in computers. A size of 2 Gigabytes is no longer unusual and it is common to find more than one fixed disk within a single machine.

The cost of the media is decreasing

slowly but this is still significant when considering the quantity of information to be copied and stored (even though the system does allow for media re-use).

There is also the problem of the length of time individual copies may take to complete. A sizeable saving in both time and expense might therefore be achieved if an alternative method of evidential security could be arranged.

Special needs of evidential authentication

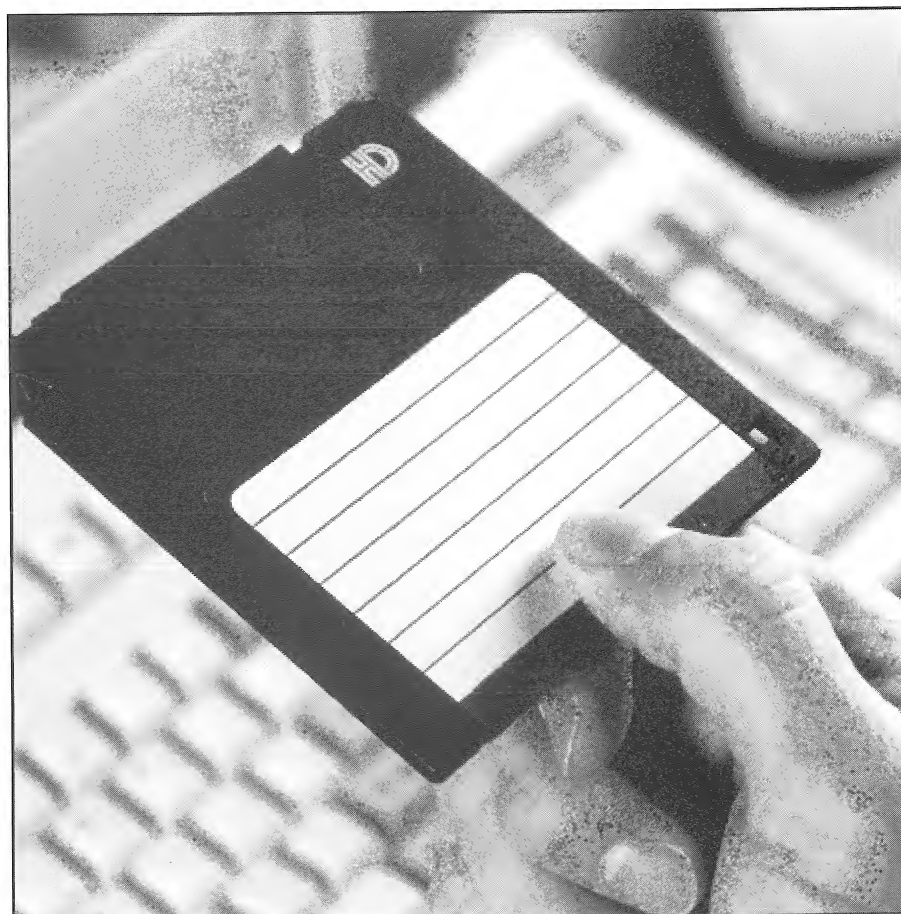
Reference to the book "Applied Cryptography" by Bruce Schneier (John Wiley & Sons Inc. ISBN 0-471-59756-

2) reveals a wealth of mathematical algorithms dealing with secure encryption, verification and authentication of computer based material.

These display varying degrees of security and complexity but all of them rely upon a "second channel" of information whereby certain elements of the encryption/decryption/authentication processes are kept secret.

This is characterised most plainly in the systems of public and private key encryption but is also apparent in the other protocols discussed and explained by Schneier. However, as good as this book is it does not adequately address the special needs of evidential integrity validation.

Consider the investigative process where computers are concerned: during an investigation it is decided that evidence may reside on a computer system. It may be possible to seize or impound the computer system but this risks vio-





lating the basic principle of “innocent until proven guilty”, by depriving an innocent party of the use of his system.

It should be perfectly possible to copy all of the information from the computer system in a manner that leaves the original system untouched and yet makes all of the contents available for forensic analysis.

When this is done, the courts may rightly insist that the copied evidence is protected from either accidental or deliberate modification and that the investigating authority should prove that this has been done! Thus it is not the content that needs protection but its integrity.

This protection takes two forms:

- A secure method of determining that the data has not been altered by even a single bit since the copy was taken.
- A secure method of determining that the copy is genuinely the one taken at the time and on the computer in question.

For the purpose of this paper, these elements are collectively referred to here as the Digital Integrity Verification and Authentication protocol (DIVA™).

It is argued that when considering forensic copies of computer contents, encryption of data is not the point at issue. Neither are the provisions of the many digital signature protocols appropriate to the requirements of evidential authentication.

Practical Considerations

It is useful to present some fundamental requirements of a forensic data collection system before we consider how these can be securely protected. These requirements were chosen to reflect my own experience of computer investigations in the UK over a number of years. Others may argue against some or all of them ...

- a) Forensic data collection should be complete and non-software specific - avoiding software traps and hidden partitioning.
- b) In operation it should be as quick and as simple as possible to avoid error or delay.
- c) It should be possible for anyone to use it with the minimum amount of training.
- d) Necessary costs and resources

should be kept to a minimum.

To meet the conditions specified in items b), c) and d) in this list, the DIVA™ protocol must be tailored to suit.

For the collection phase to remain quick and simple, the DIVA™ protocol must not add significantly to the time required for copying. Neither should there be additional (possibly complex) procedures.

The time and effort required to introduce links with Key Management agencies, trusted third parties, Key Distribution Centres and the similar paraphernalia of digital signatures and document authentication is not necessary and would add to the cost and complexity with little increase to security.

It might mean for example that only investigators issued with a valid digital signature would be able to complete copies. Who is to issue these? Where are they to be stored? How will each individual remember his own key? How can misuse of keys be detected?

The DIVA™ protocol described below is virtually a self-contained system which makes a somewhat novel use of some of the techniques described in Schneier's book (q.v.)

Quite obviously a truly self-contained encryption system cannot be cryptographically secure. However, within the DIVA™ protocol, alternative channels of security are used to provide a truly secure system but at much lower cost in time and consumables.

Practical implementation

The emphasis here is on a practical application of proven technology such that a minimum amount of reliance is placed upon the technical ability of the operator/investigator.

It must be understood that during the copying process, procedures are implemented to trap and handle hardware errors, mapping exceptions where necessary.

It must also be understood that procedures are implemented to verify that information is copied correctly.

Within the current DIBS® system, as well as the raw data content of the suspect disk drive, a copy is also taken of the high section of conventional memory

(to include any on-board ROM areas) and the CMOS contents via port access. This information is stored on each cartridge within a copy series.

Also stored on each cartridge is a reference area containing copy specific information - like CPU type and speed, hardware equipment indicators, copying drive serial number, cartridge sequence number, exhibit details and reference comments, operator name together with a unique password and the real date and time as entered by the operator.

The remainder (in fact the bulk) of each cartridge contains the information copied from the suspect drive on a sector by sector basis.

For the purposes of the DIVA™ protocol, the cartridge is divided into blocks of an arbitrarily chosen size. Blocks may contain reference, ROM, CMOS or disk data depending upon their location on the cartridge.

A pre-specified area of each cartridge is set aside to store integrity verification information for the blocks on that cartridge.

Using the analogy of a Bank Vault and Safety Deposit boxes - the storage area containing the integrity verification information pertaining to each block is referred to as a Safe Box. While the whole of the pre-specified area where the Safe Boxes are stored is referred to as the Vault.

Safe boxes and the vault

As each block is copied and verified, a hash value is generated such that a single bit change anywhere within the block would produce a different hash. The result is stored in the relevant Safe Box and copying proceeds to the next block.

Once all the blocks relevant to a particular cartridge have been copied and treated in this way, the whole group of Safe Boxes, collectively referred to as the Vault, are treated as an individual block and a Vault hash value is generated and stored in the final safe box.

The Vault is then copied to another area of the cartridge and this second copy is encrypted.

The Vault hash value for each cartridge is stored in a separate area in memory and the operator is prompted to

insert a new cartridge until the copy is completed.

The final cartridge will contain similar information to the others in the series and in addition will have the accumulated Vault hash values from all other cartridges in the series.

Once the final cartridge has been copied, the operator is prompted to insert a preformatted floppy disk into the drive used to start the DIBS® process.

All of the accumulated Vault hash values are then written to a floppy disk together with the reference details of the whole copy procedure. At least two (identical) floppy disks are created in this manner although the operator may elect to generate more if he wishes.

The floppy disks are then sealed in numbered, tamper-proof bags and both numbers are written on both envelopes. These are then shown to the owner of the computer or his legal representative and he chooses one of them.

The computer owner is then given his chosen floppy and the other is placed in secure storage. The tamper-proof envelopes are printed with instructions on their use and storage such that the computer owner is aware of the protection that he is being given.

If the computer owner or his legal representative is not available then both disks are placed in secure storage.

Security Considerations

The overall security of this system rests in the combination of security measures. These can be summarised technically as follows:

The block hash values are generated in conjunction with a one-time pad simulation. As well as providing continuity between blocks, this also negates the redundancy encountered when copying the type of data found on fixed disks - e.g. quantities of zeroes, ASCII text and fixed structures.

Thus repeat hash values are avoided and a possible birthday attack is thwarted.

The encryption of the Vault, since it only occurs at the end of each section of the copy can be accomplished using a secure encryption algorithm.

Both the prosecuting and defending parties have a secure protection against the possibility of the evidence being tampered with as long as they retain the sealed floppies. In the event of a challenge, one or both envelopes can be opened in court and verified against each other and the cartridges.

In the event of a mismatch with the cartridge, reference to the encrypted Vault stored on the cartridge will show which block on the cartridge has been altered (or even the Vault itself).



Conclusions

Having examined various alternative methods of copying suspect computers, I remain convinced that the DIBS® imaging concept with dedicated hardware remains the simplest, most secure and most practical method currently available.

Copying directly to CD-ROM is not possible without some buffer drive to enable correct data streaming, and this introduces a number of potential problem areas both with the increasingly complex hardware and evidential continuity.

It should also be noted that CD-ROM technology was originally developed for audio requirements and the current reliability when storing digital data is extremely suspect.

Copying to tape is less expensive but the viability of data stored for long periods (in many cases - years) particularly if unattended is also extremely suspect.

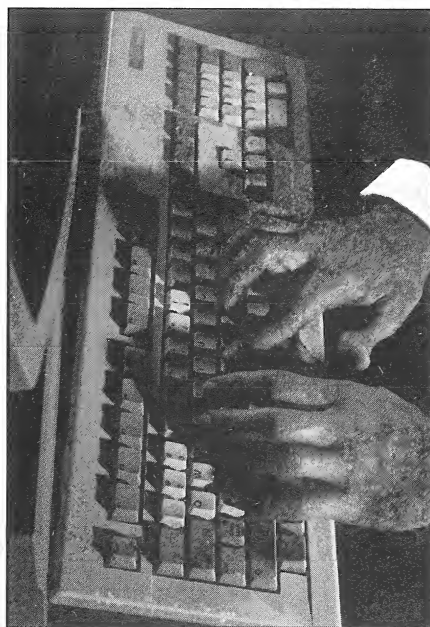
Both of these methods also have additional problems of data verification during and after the copy process. Software copying packages intended for use on non-specific peripheral storage devices raise problems of technical support and hardware matching.

The problems that were originally anticipated with re-writable media have not materialised and the advantages far outweigh the disadvantages. The process of copying fixed disks at BIOS level has enabled DIBS® to avoid problems with operating systems and access control mechanisms whilst the drive restoration process has proven capable of dealing with all currently available operating systems on the PC platform.

In spite of these observations, as far as I am aware, no forensic copying system in current use offers equal protection to both the investigator and the computer owner. Note that this protection does not depend upon how securely the copy cartridges are stored, nor on the relative security attending the storage of the floppy disks.

Rather it depends upon the combination of all three and the technical security of the encryption mechanisms.

The DIVA™ protocol is not intended



to supplant the existing dual-copy practice being used by most UK Police Forces. My intention is to provide an equally secure alternative with due consideration of costs and resources.

The presence of a cryptographically secure verification of the contents of each cartridge is a vital addition in this age of high-tech crime. It may even be thought useful by some operators to use both the dual-copy practice and the DIVA™ protocol since this provides combined security of data contents with integrity verification and security for the computer owner.

It is accepted that no security system can be 100% proof against subversion. However, careful consideration and detailed research have produced the DIVA™ protocol described above and I consider this to be as secure as is practically possible for the material being protected.

To successfully subvert the DIVA™ protocol, it would be necessary to:

- Alter the data on the cartridge - either in a manner which ensures that the relevant data block produces the same hash value - or:

- Recalculate the relevant hash value and insert it into the Vault and
- Recalculate all the subsequent derivative hash values and
- Recalculate and rewrite the relevant encrypted block and

- Break the seals on the relevant DIVA™ floppy disks - rewrite the data and repair the seals.

All without detection!

An alternative attack might be (if the machine in question was available) to alter the data on the machine and then re-DIBS® it. This would require:

- The original DIBS® drive.
- The original password known only to the copying officer (and severally encrypted on each cartridge in the series).
- Exact knowledge of the date time settings within the computer at the time of the original copy.
- A similarly numbered tamper proof bag upon which the defendant's signature would be forged - or the original bag opened and resealed with the new floppy inside.

Any discrepancies between the defendant's floppy disk and that of the investigators could be examined and analysed to determine whether such discrepancies disqualified any or all of the copied data.

The digital integrity of the floppy disk and the physical integrity of the tamper-proof bag in this case being the arbiters of whether such discrepancies had been deliberately manufactured.

The inclusion of the encryption phase means that the digital integrity of any element in the chain (cartridges and floppies) can be verified independently of the others. It is thus useless for a defendant to destroy his floppy disk in the hope that its absence will assist any challenge to the DIVA™ protocol.

Full technical details of the DIVA™ protocol have been filed with the UK Patent Office.

The original paper on this subject was written by Jim Bates, Technical Director, Computer Forensics Ltd. The company can be contacted at: info@computer-forensics.com. Or visit the Web site at <http://www.computer-forensics.com>.

Notice Board

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

Events

12th International Congress on Criminology

Crime and Justice in a Changing World: Asian and Global Perspectives

24-29 August 1998
Seoul, Korea

The 12th ICC will explore and discuss current trends and research in the fields of criminology and criminal justice systems. Plenary sessions will feature keynote speeches by world renowned criminologists.

Topics will include organised and white collar crime, corrections, historical and comparative perspectives on criminology.

The 12th ICC will also feature The World Criminology Exhibition 1988. Hosted by the Korean Institute of Criminology. Organised by the International Society for Criminology.

Contact: KIC
Tel: (822) 571 0365/5288
Fax: (822) 571 7487/5290

Practical NetWare Security

10 September 1998
Abingdon, Oxfordshire, UK

This workshop offers the opportunity to experience actual attacks on networks and shows the attendees how to defend against them.

Participants work in a live multi-server network domain with personal supervision (one PC per participant, 16 participants maximum).

The workshop is structured as a full day course with emphasis on practical learning. Participants will gain experience which would otherwise be obtained only as the result of an actual disaster.

Contact: Daniel Trotman
Sophos Plc
Tel: +44(0)1235 559933
Fax: +44(0)1235 559935

Risk Management and Internal Audit in Telecoms

16 and 17 September 1988
Strand Palace Hotel, London

Developing a risk aware culture and optimising methods for tackling IT fraud and reputation risks.

Contact: Vision in Business Ltd
Tel: +44(0)171 839 8391
Fax: +44(0)171 839 3777

Securing the Future

26 and 27 September 1988
Basingstoke, Hampshire, UK

The keynote opening speech of this annual conference of the International Institute of Security will be given by the Assistant Chief Constable of Hampshire, UK.

Contact: Paula Tarr,
International Institute of Security

Tel: +44(0)1803 663275
Fax: +44(0)1803 663251

Second DIBS User Group - Newcastle

The second DIBS® user group was hosted by Bob Russell and Frank Nesbitt at the Northumbria Police Headquarters in Newcastle.

The two-day meeting included an open session for users from across Britain and further afield to discuss any tips, problems or suggestions they had after using the DIBS® equipment.

DS Nigel Jones from Kent Police gave an in-depth presentation on the Computer Evidence Protocol. (Editor's note - the Journal will be carrying a special feature on this subject).

Hosts Bob and Frank surpassed themselves with the social events - an Italian meal followed by a night of dancing in a floating nightclub - with the result that there were a few jaded faces the next day.

The second day featured a talk by Computer Forensics, followed by a question and answer session, with items discussed including retrieving evidence from Zip disks, Internet investigations and examining Apple Mac computers.

The next DIBS User Group will be held in Dublin later this year. Contact Dave Lattimore on +44 (0)1189 504611 for more information.

Subscription Form

Send completed form to **International Journal of Forensic Computing, Colonnade House, High Street, Worthing, West Sussex BN11 1NZ, UK.**

Please enter my subscription to International Journal of Forensic Computing at the rate of:

☐ UK £186.00 ☐ Europe £216 ☐ International £236.00

Name..... Position.....

Company..... Address.....

Postcode/Zip..... Country.....

Tel..... Fax.....

☐ Cheque attached (make payable to
International Journal of Forensic Computing)

Cardholder's name.....

☐ Please invoice my company quoting purchase order no.....

Card No.

Expiry date.....

Signature.....

☐ Please debit my credit card:
VISA/Mastercard/AMEX

Date.....



International Journal of
FORENSIC COMPUTING™



Published by
Computer Forensic Services Ltd.